ThoughtSpot

# ThoughtSpot Cloud: Data Transfer Impact Assessment

**January 2024**

## Introduction

This Data Transfer Impact Assessment White Paper assists ThoughtSpot customers in conducting their own risk assessment for the transfer of personal data in connection with the use of ThoughtSpot Cloud products, in view of the Court of Justice for the European Union's "Schrems II" ruling and the recommendations from the European Data Protection Board.

Under the European data protection laws, personal data may not be transferred outside of Europe (defined below) unless: (i) the importing country has been deemed adequate by the relevant governmental body; or (ii) the data exporter has appropriate safeguards in place to ensure that personal data transferred is subject to an adequate level of protection. These safeguards are referred to as "transfer mechanisms." The information below details the direct and onward data transfers and transfer mechanisms applicable to ThoughtSpot customers.

## Data Transfer Details

ThoughtSpot transfers personal data out of the EEA, UK, and Switzerland (together, "Europe") to: (1) countries holding adequacy status under the European data protection law; and (2) countries without adequacy decisions and in reliance on Standard Contractual Clauses, as outlined below.

| Europe/EEA and Adequate Countries | Countries without Adequacy Decisions |
|---|---|
| **United Kingdom and United States*** ThoughtSpot, Inc. and, its affiliate Mode Analytics, Inc., participate in and certify compliance with the Data Privacy Framework Principles and, therefore, can rely on the adequacy decision to receive EU personal data. You can find our Data Privacy Framework Certification here and our Data Privacy Framework Policy here. here. | **Australia and India** Where adequacy does not apply, ThoughtSpot continues to rely on the Standard Contractual Clauses ("SCCs") as a transfer mechanism, see below for more details. |

*For organizations participating in the Data Privacy Framework

Our analysis of transfers to countries without adequacy decisions is described below.

| Australia | |
|---|---|
| **Purpose for transfer and any further processing** | **Direct transfers:** Not Applicable. **Onward transfers:** ThoughtSpot uses Confluence for incident response and support and Jira is used for bug and ticket handling. In the unlikely event a customer includes Administrative Information containing personal data in their support request, it will be processed in Australia. |
| **Frequency of the transfer** | **Direct transfers:** Not Applicable. **Onward transfers:** Incidental. |
| **Categories of personal data transferred** | **Direct transfers:** Not Applicable. **Onward transfers:** Determined at the sole discretion of the data exporter. Please refer to our sub-processors page for more information. |
| **Sensitive data transferred (if applicable)** | **Direct transfers:** Not Applicable. **Onward transfers:** Determined at the sole discretion of the data exporter. Please refer to our sub-processors page for more information. |
| **Description of processing chain** | **Direct transfers:** Not Applicable. **Onward transfers:** Please refer to our sub-processors page for more information. |
| **Applicable transfer mechanism** | **Direct transfers:** Not Applicable. **Onward transfers:** Standard Contractual Clauses between ThoughtSpot and its sub-processors. ThoughtSpot imposes obligations on its sub-processors to implement appropriate technical and organizational measures ensuring that the sub-processing of personal data is protected to the standards required by applicable data protection laws including, without limitation, the General Data Protection Regulation. |

| Australia | |
|---|---|
| **Laws relevant to the data transfers** | Australia has several laws, legislation, and executive powers that can be used to compel companies to disclose personal data, or that enable investigative and enforcement agencies to obtain data where there is a suspected violation of law.<br><br>*Crimes Act 1914 (Cth) and the Criminal Code Act 1995 (Cth)*, which permits government agencies to collect both electronic and physical data where there are reasonable grounds to believe there is a criminal offense.<br>Surveillance Devices Act 2004 (Cth) and equivalent state and territory laws that grant authorities covert access to electronic and physical data.<br><br>*Telecommunications (Interception and Access) Act 1979 (Cth)* and Part 15 of the Telecommunications Act 1997 (Cth) grants government bodies powers to oblige telecommunications carriers, carriage service providers, and other communications providers to assist law enforcement and intelligence agencies.<br><br>For each of the above laws, there are potential extra-territorial powers that could theoretically compel those outside of Australia to assist in the investigative process. In practice, however, it is extremely unlikely that law enforcement and surveillance authorities will be able to do so without operating through existing bilateral processes, such as mutual legal assistance treaties. In practice, it can be difficult to determine how governmental authorities use their powers to conduct surveillance and collect data (and, therefore, whether it involves unnecessary or disproportionate data access in any circumstances) because government authorities are often not required to publicly report on when and how they use these powers (although independent oversight and review, including reporting to independent statutory authorities, is embedded throughout the surveillance legislation framework). In addition, not all requests for access to data and surveillance are currently subject to prior independent judicial authorization.<br><br>ThoughtSpot publishes and follows its Guidelines for Law Enforcement in responding to any government requests for data. We also publish an annual Transparency Report with information about government requests to access data. |

| India | |
|---|---|
| **Purpose for transfer and any further processing** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** ThoughtSpot may transfer customer personal data to its India affiliate/sub-processor for the purpose of assisting in the provision of the products. Please refer to our sub-processors page for more information. |
| **Frequency of the transfer** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** Continuous. |
| **Categories of personal data transferred** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** Determined at the sole discretion of the data exporter. Please refer to our sub-processors page for more information. |
| **Sensitive data transferred (if applicable)** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** Determined at the sole discretion of the data exporter. Please refer to our sub-processors page for more information. |
| **Description of processing chain** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** Please refer to our sub-processors page for more information. |
| **Applicable transfer mechanism** | **Direct transfers:** Not Applicable.<br>**Onward transfers:** Standard Contractual Clauses between ThoughtSpot and its sub-processors. ThoughtSpot imposes obligations on its sub-processors to implement appropriate technical and organizational measures ensuring that the sub-processing of personal data is protected to the standards required by applicable data protection laws including, without limitation, the General Data Protection Regulation. |
| **Laws relevant to the data transfers** | India has several surveillance, criminal, and security laws which allow government agencies to intercept and access “personal information” and “sensitive personal data or information” without obtaining their prior consent if relevant factors apply. A high-level overview of the key laws is provided below.<br><br>*The Information Technology Act, 2000* empowers government agencies to intercept any information generated, transmitted, received, or stored in any computer resource. This can be in the interest of the sovereignty, integrity of India, security, and defense of India, etc. A subsection of the act grants the central government power to authorize any government agency to monitor and collect traffic data to enhance cybersecurity, identification, analysis, and prevention of intrusion or spread of a computer containment.<br><br>*The Indian Telegraph Act, 1885* confers upon the Indian government the right to conduct surveillance over telegraph lines but only upon the occurrence of a public emergency or the interest of public safety. |

| India | |
|---|---|
| | *The Digital Personal Data Protection Act, 2023* ("DPDP Act") provides that personal information may be shared by data fiduciaries to the State/agents of the State under a legal obligation is a 'legitimate use', not requiring consent of or notice to the data principals. Further, the State/agents of the State themselves are exempted from seeking consent (and other obligations under the DPDP Act, including that of erasure of personal data in its records) while processing personal data, which is for the performance of any legal function, is in the interest of security, sovereignty and integrity of India or is to maintain public order.<br><br>Because the scope of interception and surveillance powers of Indian authorities extends to investigations carried out in respect of any persons, companies, and entities operating within India (including those doing business in India from offshore), any data recipient is potentially within the scope of criminal law enforcement and theoretically shall be obligated to share data if compelled to do so by a government authority. The CrPC applies to the territory of India and accordingly, an offshore entity is not under an obligation to comply with the request, however, if the offshore entity has a presence in India, the CrPC would extend to such operations within India.<br><br>ThoughtSpot publishes and follows its Guidelines for Law Enforcement in responding to any government requests for data. We also publish an annual Transparency Report with information about government requests to access data. |

| United States | |
|---|---|
| **Purpose for transfer and any further processing** | **Direct transfers:** ThoughtSpot has offices in the United States where our employees may access personal data for the purposes of the provision of ThoughtSpot Cloud (including ThoughtSpot Mode).<br>**Onward transfers:** ThoughtSpot transfers personal data to its sub-processors for the purpose of assisting in the provision of our services. Please refer to our sub-processors page for more information. |
| **Frequency of the transfer** | **Direct transfers:** Continuous.<br>**Onward transfers:** Continuous. |
| **Categories of personal data transferred** | **Direct transfers:** As detailed in ThoughtSpot DPA.<br>**Onward transfers:** Please refer to our sub-processors page for more information. |
| **Sensitive data transferred (if applicable)** | **Direct transfers:** None.<br>**Onward transfers:** Please refer to our sub-processors page for more information. |
| **Length of processing chain** | **Onward transfers:** Please refer to our sub-processors page for more information. |
| **Applicable transfer mechanism** | **Direct transfers:** ThoughtSpot's DPF Certification for the contractual relationship between ThoughtSpot (including Mode) and its customers.<br>**Onward transfers:** Standard Contractual Clauses between ThoughtSpot (including Mode) and its sub-processors. ThoughtSpot imposes obligations on its sub-processors to implement appropriate technical and organizational measures ensuring that the sub-processing of personal data is protected to the standards required by applicable data protection laws. |
| **Identifying laws and practices relevant in light of all circumstances of the transfer** | The following US laws were identified by the Court of Justice of the European Union in Schrems II as being potential obstacles to ensuring essentially equivalent protection for personal data in the US:<br><br>*FISA Section 702 ("FISA 702")*, which allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering.<br><br>*Executive Order 12333 ("EO 12333")*, authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. It provides authority for US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire, and other electromagnetic means. |

| United States | |
|---|---|
| | The following US laws were identified by the Court of Justice of the European Union in Schrems II as being potential obstacles to ensuring essentially equivalent protection for personal data in the US:<br><br>*FISA Section 702 ("FISA 702")*, which allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering.<br><br>*Executive Order 12333 ("EO 12333")*, authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. It provides authority for US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire, and other electromagnetic means.<br><br>Further information about these U.S. surveillance laws can be found in the U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II whitepaper from September 2020. For the CLOUD Act, please refer to What is the CLOUD Act? by BSA Software Alliance outlining the scope of the CLOUD Act. |

# DATA PRIVACY FRAMEWORK

In 2023, with the US Data Privacy Framework, Europe introduced the adequacy framework for US companies that self-certify under the DPF. Critical to the adoption of the adequacy decision was the updated US legal framework, e.g. "Enhancing Safeguards for United States Signals Intelligence Activities", which was signed by President Biden in October 2022 and is accompanied by regulations issued by the United States Attorney General. These safeguards were adopted to address the issues raised by the Court of Justice in its Schrems II judgment.

For Europeans whose personal data is transferred to the US, the Executive Order provides for:

- Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;
- Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and
- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

ThoughtSpot, Inc. and its US affiliate Mode Analytics, Inc. participate in and certify compliance with the United States Data Privacy Framework. Our US entities can rely on the adequacy decision to receive EU personal data. You can find more information in our Data Privacy Framework Policy.

ThoughtSpot publishes and follows ThoughtSpot's Guidelines for Law Enforcement Requests in responding to any government requests for data. We also publish an annual Transparency Report with information about government requests to access data. As of the date of this Whitepaper, ThoughtSpot (including Mode Analytics) have not received any such requests.